(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 168 817 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.01.2002 Bulletin 2002/01

(51) Int Cl.7: H04N 1/32

(21) Application number: 01305333.5

(22) Date of filing: 19.06.2001

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 20.06.2000 JP 2000184866

(71) Applicant: MATSUSHITA ELECTRIC INDUSTRIAL
CO., LTD.
Kadoma-shi, Osaka 571-8501 (JP)

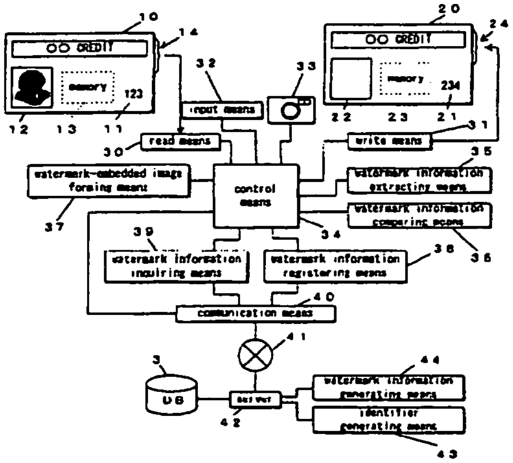
(72) Inventors:
- Kawaguchi, Yuichi
Kadoma-shi, Osaka 571-8501 (JP)
- Tsumori, Shinichi
Kadoma-shi, Osaka 571-8501 (JP)
- Shimizu, Yuji
Kadoma-shi, Osaka 571-8501 (JP)
- Katsura, Takashi
Kadoma-shi, Osaka 571-8501 (JP)
- Inoue, Hisashi
Kadoma-shi, Osaka 571-8501 (JP)

(74) Representative: Shelley, Mark Raymond et al
K R Bryer & Co., 7 Gay Street
Bath BA1 2PH (GB)

(54) Authenticating system, personal certification issuing system, personal certificate and methods therefor

(57) A justification/authentication personal certificate system stores in a remote database (3) a counterpart of an identifier (11) and a digital watermark contained in the personal certificate (10). The personal certificate includes the digital watermark embedded in an authentic image (12) such as a facial photograph, a retinal scan, or a fingerprint. When the personal certificate is used. the authentic image is read from the personal certificate, and the digital watermark information is extracted. The digital watermark information and the identifier are compared with the counterparts stored in the database. If the extracted digital watermark information is identical to the information in the database, then the personal certificate is judged to be unjustifiable. In one embodiment, at least one of the identifier and digital watermark are changed each time the system justifies the personal certificate.

Fig. 1


10
OO CREDIT
memory
123
14
12
13
11
32
input means
33
20
24
OO CREDIT
memory
234
22
23
21
31
30
read means
write means
35
watermark-embedded image forming means
control means
watermark information extracting means
watermark information comparing means
37
39
34
38
36
watermark information inquiring means
watermark information registering means
40
communication means
41
3
44
DB
server
watermark information generating means
identifier generating means
42
43

Printed by Jouve, 75001 PARIS (FR)

means and said digital watermark information generated by said watermark information generating means in said database, an image input means for inputting a raw authentic image, a watermark-embedded image forming means for forming a watermark-embedded authentic image in which said digital watermark is embedded on said authentic image input by said image input means, and a personal certificate that readably carries said authentic image generated by said watermark-embedded image forming means and said identifier generated by said identifier generating means.

[0013] According to a further aspect of the invention, there is provided a personal certificate comprising: a unique identifier, an authentic image of an authorized user of said personal certificate, said authentic image being viewable by eye, said authentic image containing embedded therein digital watermark information corresponding to said identifier, and means for permitting communication of said identifier and said digital watermark information to a database remote from said personal certificate.

[0014] Preferably, digital watermark information embedded in an authentic image is stored not only on the authentic image of a personal certificate but also on a database, and therefore only justifiable use is permitted following a comparison of the digital watermark information stored in the database and the digital watermark information extracted from the personal certificate.

[0015] For example, since the database itself is not modified even if digital watermark information is embedded expertly in the facial photograph of a personal certificate stolen by the offender B, the comparison with the database fails, and the illegality of the offender B is exposed, that is to say, compared with the case in which security depends only on the authentic image of the personal certificate, security can be greatly improved.

[0016] Preferably, the digital watermark stored in the information carrier can be read as digital data, and therefore the digital watermark information can be accurately compared.

[0017] Preferably, the information carrier is a semiconductor memory or a magnetic material, and therefore data can be stored without greatly increasing the weight of the personal certificate.

[0018] Preferably, the authentic image is printed on printed matter, and therefore the personal certificate is thinner and lighter.

[0019] Preferably, random values are included in the digital watermark information. Therefore, persons who attempt falsification or alteration cannot predict the random portion of the information. This increases the difficulty of falsification.

[0020] Preferably, the digital watermark information embedded in the facial photograph information of the database and of the personal certificate is updated whenever necessary or desirable. Therefore, infallible measures can be taken against falsification.

[0021] Preferably, the database is located at a distance from the place where the personal certificate is used. The data is communicated through a communication network. Thus, the digital watermark information does not leak out as long as access to the database is prevented. Therefore, the security of the system is improved.

[0022] Various embodiments of the invention will now be more particularly described, by way of example, with reference to the accompanying drawings, in which:

Fig. 1 is a block diagram of a system according to a first embodiment of the present invention.

Fig. 2 is a block diagram of a system according to a second embodiment of the present invention.

Fig. 3 is a flowchart showing an issuing process according to the first embodiment of the present invention.

Fig. 4 is a flowchart showing an authentication process of the present invention.

Fig. 5 schematically shows the relationship among a personal certificate, an identifier, a digital watermark, and a database of the same.

[0023] Embodiments of the present invention are described hereinafter with reference to the accompanying drawings. First, prior to the description of each embodiment, the relationship among an identifier, digital watermark information, and a database according to the present invention is roughly described with reference to Fig. 5. A case where the photographic image of a face is used as an authentic image is primarily described below.

[0024] As shown in Fig. 5, a personal certificate 5 includes an identifier 1 and an authentic image 4. There is a one-to-one relationship between the identifier 1 and digital watermark information 2 which are stored in a database 3. In this example, for purposes of description, and not as a limitation, the identifier 1 is "123", and the digital watermark information 2 is "hogehoge".

[0025] Referring to Fig. 1, a system according to the first embodiment of the present invention employs a personal certificate 10 shown at the upper left of Fig. 1. The personal certificate 10 is one that has been issued, and is used for authentication. A personal certificate 20 shown at the upper right of Fig. 1 is being prepared for issue, but has not yet been completed for issue.

[0026] The completed and issued personal certificate 10 has a display part 12 in which a photograph of a face or the like is displayed, a memory 13 as an information carrier, and an identifier 11(in this embodiment, "123").

[0027] The personal certificate 10 further has an input-output port 14 to access the memory 13. If the capacity is large enough to store an image, a magnetic material, such as a magnetic strip, may be used as an ing aspects of the system are identical to the structure of Fig. 1.

[0045] Next, the flow of a process for issuing the personal certificate is described hereinafter with reference to Fig. 3. In the second embodiment, the technique of the reading/writing of the authentic image merely differs in the processing itself, and therefore the first embodiment is primarily described.

[0046] First, the operator of this system or the owner of the personal certificate inputs necessary personal information to the system using the input means 32 (step 1). Thereafter, at step 2, the owner's face, corneal pattern, fingerprint, or other identifying pattern, is photographed with the digital camera 33, scanner, or other device, to acquire an authentic image.

[0047] At step 3, the control means 34 connects to the server 42 through the communication network 41 using the communication means 40.

[0048] Thereafter, at step 4, the control means 34 requests the server 42 to generate an identifier and watermark information corresponding to this identifier through the communication means 40.

[0049] In response to this, the identifier generating means 43 on the server 42 side accesses the database 3, and generates a new identifier that has not yet been assigned. The watermark information generating means 44 generates watermark information corresponding to this new identifier. The identifier and the watermark information are transmitted to the control means 34 (step 5).

[0050] The control means 34 receives them, and requests the watermark information registering means 38 to register the received identifier and watermark information on the database 3 (step 6). In response to this demand, the server 42 stores the information in the database 3. Thereafter notification is transmitted to the control means 34 that the registration has been completed (step 7).

[0051] Upon receiving this notification, the control means 34 releases the connection with the server 42 (step 8), and gives the received watermark information and the authentic image obtained from the digital camera 33 to the watermark-embedded image forming means 37, and thereby a watermark-embedded image is formed (step 9).

[0052] At step 10, the watermark-embedded image formed as described above is transmitted to the write means 31. The write means 31 writes this image into the memory 23 through the input-output port 24, and the authentic image is displayed on the display part 22 when necessary. This completes the issuing process.

[0053] Next, the authentication process is described with reference to Fig. 4. The personal certificate 10 that has been issued is inserted into the read means 30. First, the read means 30 reads an identifier 11 (herein "123") from the personal certificate 10 (step 20). The identifier may be input by any convenient device such as, for example, with the input means 32.

[0054] Thereafter, at step 21, the read means 30 reads the authentic image that is stored in the memory 13 and in which digital watermark information is surely embedded, through the input-output port 14.

[0055] Thereafter, at step 22, the control means 34 transmits the obtained authentic image to the watermark information extracting means 35, and causes the extracting means 35 to extract watermark information from the authentic image. If this extraction fails (step 23), the control means 34 judges that the personal certificate 10 is unjustifiable (step 24), and terminates the processing.

[0056] On the other hand, if the extraction of the watermark information succeeds, the control means 34 connects to the server 42 through the communication means 40 (step 25).

[0057] The control means 34 transmits the identifier 11 that has been read from the personal certificate to the watermark information inquiring means 39, and causes the inquiring means 39 to acquire the watermark information corresponding to the identifier 11 (step 26).

[0058] When receiving this inquiry, the server 42 retrieves the watermark information corresponding to the identifier in the database 3. If the watermark information is not found, the server 42 sends a message that the corresponding information is not found. If the watermark information is found, the server 42 returns the found watermark information to the control means 34 (step 27).

[0059] When the control means 34 receives the information from the server 42, the control means 34 releases the connection (step 28). If the control means 34 receives the message that the watermark information is not found (step 29), it is judged that the personal certificate 10 is unjustifiable (step 24), and the processing is terminated.

[0060] On the other hand, when receiving the watermark information, the control means 34 transmits the watermark information extracted by the watermark information extracting means 35 and the watermark information received from the server 42 at this time to the watermark information comparing means 36 for a comparison. If the watermark information from the two sources are found to be non-identical in the comparison made by the watermark information comparing means 36, the control means 34 determines that the personal certificate 10 is unjustifiable (step 24), and terminates the processing.

[0061] On the other hand, if the watermark information from the two sources are found to be identical in the comparison, the control means 34 determines that the personal certificate 10 is justifiable (step 31), and completes the processing.

[0062] Preferably, when the watermark is judged to be justifiable, the same process as the main part of Fig. 3 is carried out once again at step 32, and the watermark information corresponding to this identifier is updated (step 32). As a matter of course, the update means updates both the digital watermark embedded in the authentic image of the personal certificate 10 and the dig-

(38) for storing said identifier generated by said identifier generating means and said digital watermark information generated by said watermark information generating means in said database;
an image input means (32, 33) for inputting a raw authentic image;
a watermark-embedded image forming means (37) for forming a watermark-embedded authentic image in which said digital watermark is embedded on said authentic image input by said image input means; and
a personal certificate (10) that readably carries said authentic image generated by said watermark-embedded image forming means and said identifier generated by said identifier generating means.

9. The personal certificate issuing system of claim 8, wherein:

said personal certificate includes an information carrier (13) for storing said authentic image; and
said authentic image includes a digital watermark embedded in said authentic image stored in said information carrier.

10. The personal certificate issuing system of claim 9, wherein said information carrier is at least one of a semiconductor memory and a magnetic material.

11. The personal certificate issuing system of claim 9 wherein:

said information carrier includes said authentic image being a printed authentic image affixed to said personal certificate; and
said read means reads said printed authentic image.

12. The personal certificate issuing system of claim 8, wherein at least one of said identifier and said digital watermark information includes an element that is randomly generated.

13. The personal certificate issuing system of claim 8, wherein said digital watermark information stored in said database and embedded in said authentic image of said personal certificate are updated at a predetermined time.

14. The personal certificate issuing system of claim 13, wherein said predetermined time includes each time said system correctly justifies an authentic image.

15. The personal certificate issuing system of claim 8, further comprising:

a communication device for communicating said watermark information between said watermark information inquiring means and said database.

16. A personal certificate (10) comprising:

a unique identifier (11);
an authentic image (12) of an authorized user of said personal certificate;
said authentic image being viewable by eye;
said authentic image containing embedded therein digital watermark information corresponding to said identifier; and
means for permitting communication (40, 41) of said identifier and said digital watermark information to a database (3) remote from said personal certificate.

17. A method for issuing a personal authentication certificate; the said method comprising the steps of:

generating an identifier (11) unique to a personal certificate (10);
generating data relating to a digital watermark for the said identifier;
storing data relating to the said identifier, digital watermark and personal certification in relation to each other;
inputting an image to be associated with the said personal certification;
processing the said image with the said watermark data to form a watermark-embedded authentication image (12) for the said personal certificate.

18. A method for authenticating a personal authentication certificate; the said method comprising the steps of:

reading at least an authentication image (12) from a personal authentication certificate (3);
processing the said authentication image (35) to extract data relating to watermark embedded in the said image;
comparing the said extracted embedded watermark data with watermark data stored in a data storage means (11) in relation to an identifier (11) for the said personal authentication certificate;
determining whether the said extracted embedded watermark data corresponds with the said stored watermark data (36), whereby to authenticate the personal authentication certificate.

Fig. 1

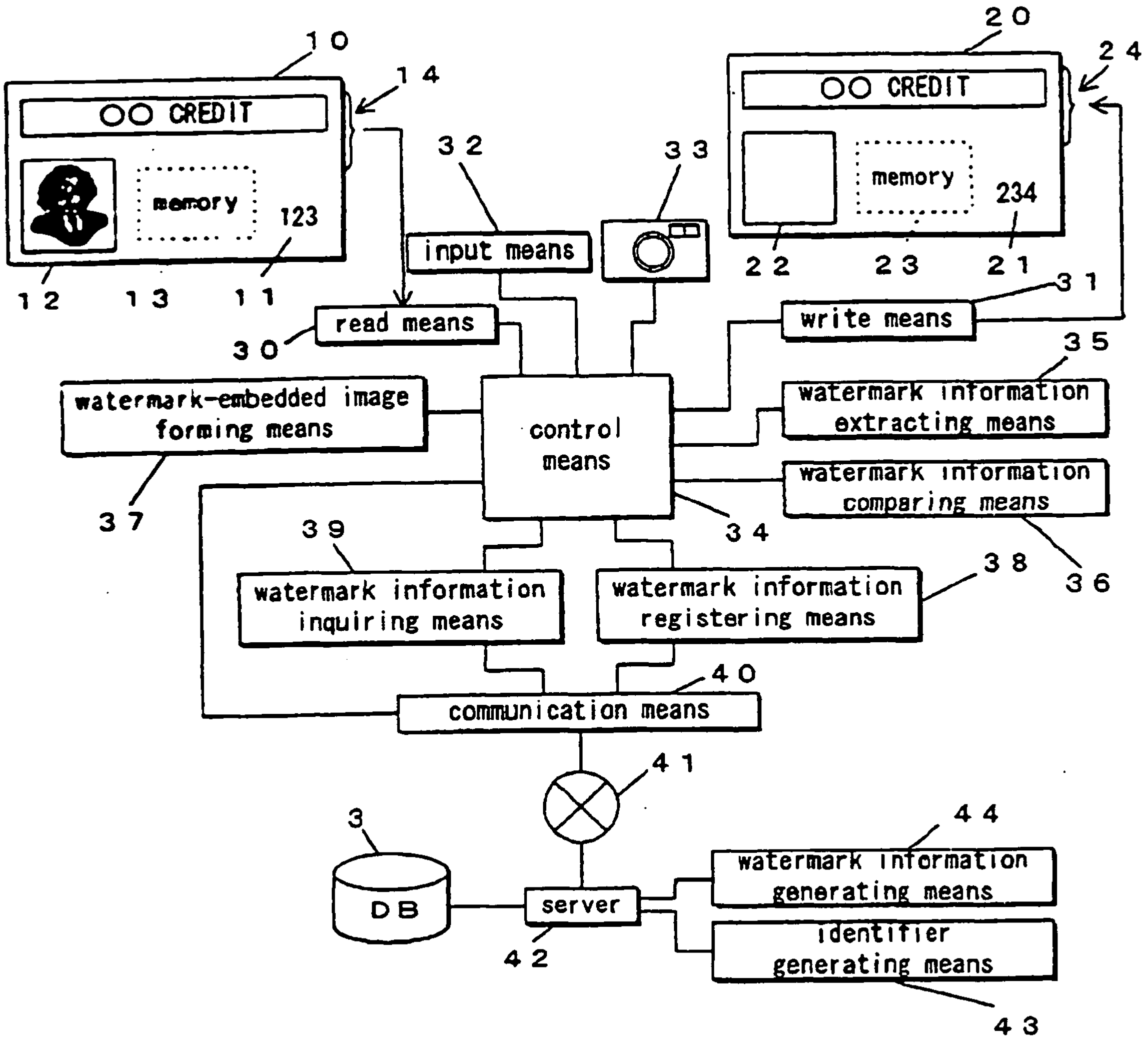

10
OO CREDIT
memory
123
14
12
13
11
20
OO CREDIT
memory
234
24
22
23
21
32
input means
33
read means
30
write means
31
35
watermark-embedded image forming means
control means
watermark information extracting means
watermark information comparing means
37
34
36
39
watermark information inquiring means
watermark information registering means
38
40
communication means
41
3
DB
server
42
44
watermark information generating means
identifier generating means
43

Fig. 3

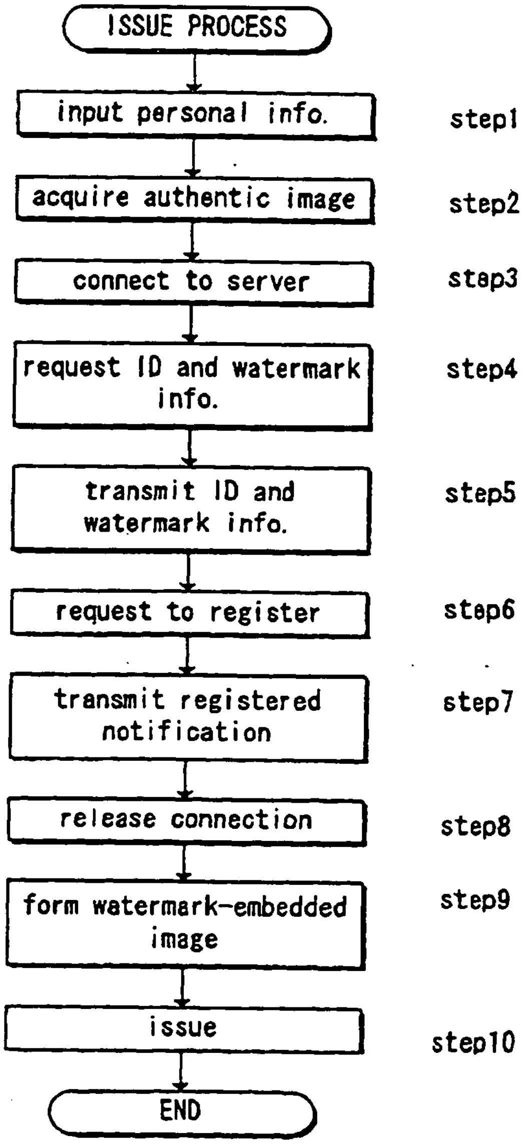
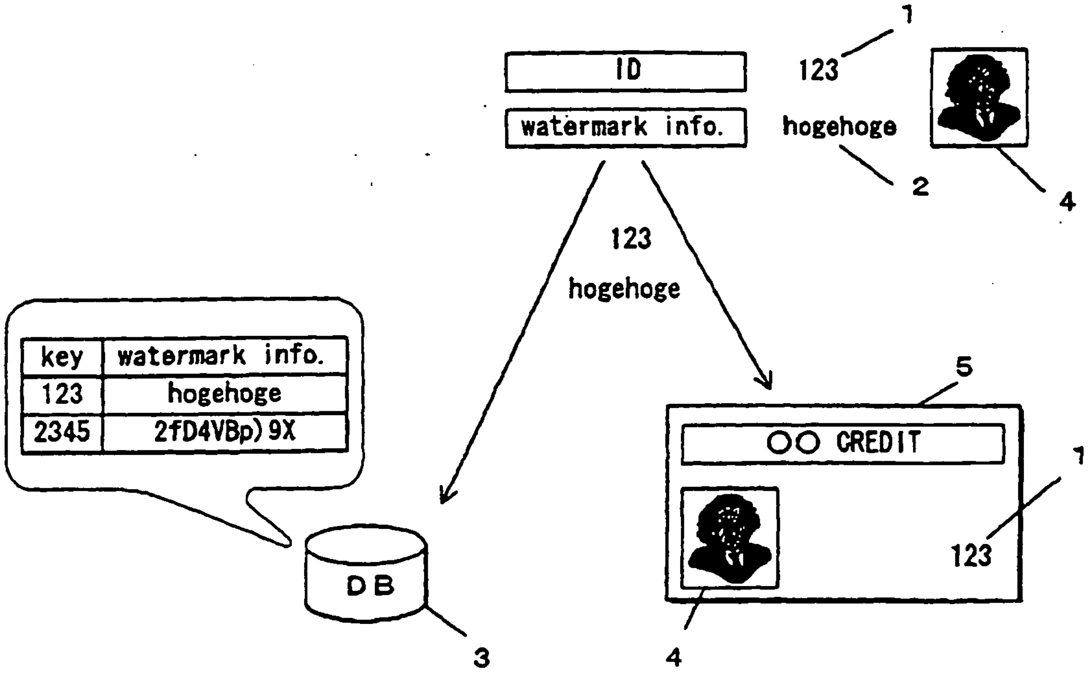

ISSUE PROCESS
input personal info.
step1
acquire authentic image
step2
connect to server
step3
request ID and watermark info.
step4
transmit ID and watermark info.
step5
request to register
step6
transmit registered notification
step7
release connection
step8
form watermark-embedded image
step9
issue
step10
END

Fig. 5



key	watermark info.
123	hogehoge
2345	2fD4VBp) 9X

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 168 817 A3

(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
12.03.2003 Bulletin 2003/11

(51) Int Cl.7: H04N 1/32

(43) Date of publication A2:
02.01.2002 Bulletin 2002/01

(21) Application number: 01305333.5

(22) Date of filing: 19.06.2001

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 20.06.2000 JP 2000184866

(71) Applicant: MATSUSHITA ELECTRIC INDUSTRIAL
CO., LTD.
Kadoma-shi, Osaka 571-8501 (JP)

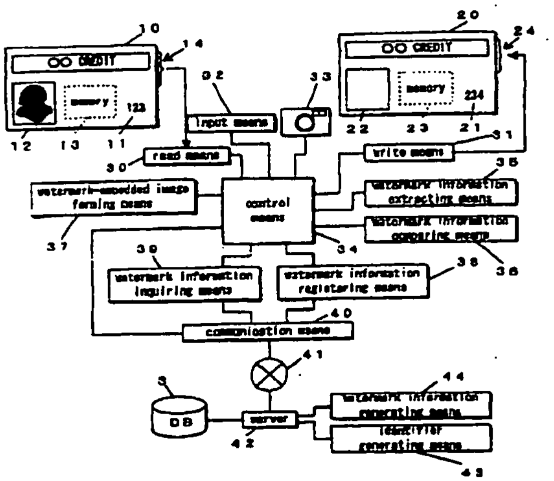
(72) Inventors:
- Kawaguchi, Yuichi
Kadoma-shi, Osaka 571-8501 (JP)
- Tsumori, Shinichi
Kadoma-shi, Osaka 571-8501 (JP)
- Shimizu, Yuji
Kadoma-shi, Osaka 571-8501 (JP)
- Katsura, Takashi
Kadoma-shi, Osaka 571-8501 (JP)
- Inoue, Hisashi
Kadoma-shi, Osaka 571-8501 (JP)

(74) Representative: Shelley, Mark Raymond et al
K R Bryer & Co.,
7 Gay Street
Bath BA1 2PH (GB)

(54) **Authenticating system, personal certification issuing system, personal certificate and methods therefor**

(57) A justification/authentication personal certificate system stores in a remote database (3) a counterpart of an identifier (11) and a digital watermark contained in the personal certificate (10). The personal certificate includes the digital watermark embedded in an authentic image (12) such as a facial photograph, a retinal scan, or a fingerprint. When the personal certificate is used, the authentic image is read from the personal certificate, and the digital watermark information is extracted. The digital watermark information and the identifier are compared with the counterparts stored in the database. If the extracted digital watermark information is identical to the information in the database, then the personal certificate is judged to be unjustifiable. In one embodiment, at least one of the identifier and digital watermark are changed each time the system justifies the personal certificate.

Fig. 1


10
14
OO CREDIT
memory
123
12
13
11
32
input means
33
20
24
OO CREDIT
memory
234
22
23
21
31
write means
30
read means
35
watermark information extracting means
watermark-embedded image forming means
control means
watermark information comparing means
37
39
34
36
38
watermark information inquiring means
watermark information registering means
40
communication means
41
3
44
watermark information generating means
DB
server
identifier generating means
42
43

Printed by Jouve, 75001 PARIS (FR)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 30 5333

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

16-01-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9636163 A	14-11-1996	US 5832119 A	03-11-1998
		US 5748783 A	05-05-1998
		US 5841978 A	24-11-1998
		AT 230539 T	15-01-2003
		AT 216546 T	15-05-2002
		AU 6022396 A	29-11-1996
		CA 2218957 A1	14-11-1996
		DE 69620751 D1	23-05-2002
		DE 69620751 T2	31-10-2002
		EP 1003324 A2	24-05-2000
		EP 1049320 A1	02-11-2000
		EP 1137251 A2	26-09-2001
		EP 0824821 A2	25-02-1998
		JP 2002504272 T	05-02-2002
		WO 9636163 A2	14-11-1996
		US 2002164049 A1	07-11-2002
		US 6111954 A	29-08-2000
		US 6438231 B1	20-08-2002
		US 5862260 A	19-01-1999
		US 2001055407 A1	27-12-2001
		US 2001010730 A1	02-08-2001
		US 2001016051 A1	23-08-2001
		US 2002067844 A1	06-06-2002
		US 2002118831 A1	29-08-2002
		US 2002090112 A1	11-07-2002
		US 5841886 A	24-11-1998
		US 2002090114 A1	11-07-2002
		US 2002136430 A1	26-09-2002
		US 2002170966 A1	21-11-2002
		US 2002188841 A1	12-12-2002
		US 6324573 B1	27-11-2001
		US 6311214 B1	30-10-2001
		US 6408331 B1	18-06-2002
		US 6286036 B1	04-09-2001
		US 6411725 B1	25-06-2002
		US 6122403 A	19-09-2000
		US 2001032251 A1	18-10-2001
		US 2002016816 A1	07-02-2002
		US 2002029253 A1	07-03-2002
		US 2002078146 A1	20-06-2002
		US 2002009208 A1	24-01-2002
US 5354097 A	11-10-1994	NL 9001368 A	02-01-1992
		AT 122968 T	15-06-1995
		CA 2085113 A1	16-12-1991
		DE 69110044 D1	29-06-1995

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82